CLAIMS

1. A apparatus for detecting adversarial activity on a network, comprising:

a memory adapted to store a host table;

a key exchanger adapted to derive a cipher key;

a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;

a mapping device adapted to map the address to the host table; and

an actuator adapted to trigger a security device when the address does not match an entry in the host table.

2. An apparatus as set forth in Claim 1, wherein the security device is a logging device adapted to log the data packet.

3. An apparatus as set forth in Claim 1, wherein the security device is adapted to signal an alarm when triggered.

Express Mail Label No. EL029404766US

4. An apparatus as set forth in Claim 1, further comprising:

a host resolution device adapted to derive the host table using an address resolution protocol.

5. An apparatus as set forth in Claim 1, further comprising:

a network device adapted to place the data packet onto a network when the address maps to the host table.

6. A method for detecting adversarial activity on a network, comprising:

storing a host table;

deriving a cipher key;

translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;

mapping the address to the host table; and

triggering a security device when the address does not match an entry in the host table.

7. A method as set forth in Claim 6, further comprising:

logging the data packet when the address does not match an entry in the host table.

8. A method as set forth in Claim 6, further comprising:

signaling an alarm when the security device is triggered.

9. A method as set forth in Claim 6, further comprising:

deriving the host table using an address resolution protocol.

10. A method as set forth in Claim 6, further comprising:

placing the data packet onto a network when the address maps to the host table.

11. A device for detecting adversarial activity on a network, comprising:

means for storing a host table;

means for deriving a cipher key;

means for translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;

means for mapping the address to the host table;

and

means for triggering a security device when the address does not match an entry in the host table.

12. A device as set forth in Claim 11, further comprising:

means for logging the data packet when the address does not match an entry in the host table.

13. A device as set forth in Claim 11, further comprising:

means for signaling an alarm when the security device is triggered.

14. A device as set forth in Claim 11, further comprising:

means for deriving the host table using an address resolution protocol.

15. A device as set forth in Claim 11, further comprising:

means for placing the data packet onto a network when the address maps to the host table.

16. A bastion host adapted for processing packet header information of a data packet, the bastion host being operable to:

store a host table;

derive a cipher key;

translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;

map the address to the host table; and

trigger a security device when the address does not match an entry in the host table.

17. The bastion host as set forth in Claim 16, the bastion host being further operable to log the data packet when the address does not match an entry in the host table.

18. The bastion host as set forth in Claim 16, the bastion host being further operable to signal an alarm when the security device is triggered.

19. The bastion host as set forth in Claim 16, the bastion host being further operable to deriving the host table using an address resolution protocol.

20. The bastion host as set forth in Claim 16, the bastion host being further operable to place the data packet onto a network when the address maps to the host table.

Docket No. 00-4045